ОБЩИЙ РЕГЛАМЕНТ ЕС ПО ЗАЩИТЕ ДАННЫХ И РОССИЙСКИЕ ОПЕРАТОРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОБЩИЙ РЕГЛАМЕНТ ЕС ПО ЗАЩИТЕ ДАННЫХ И РОССИЙСКИЕ ОПЕРАТОРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общий регламент по защите данных (General Data Protection Regulation), принятый Европейским парламентом 17 декабря 2015 г. (далее - «Регламент»), вступает в силу 25 мая 2018 г. и заменит Директиву ЕС по защите данных 95/46/ЕС.

По общему правилу, Регламент будет иметь прямое действие в государствах-членах Европейского союза (ЕС) без необходимости имплементации его положений на уровне национального законодательства. Действие Регламента также будет распространяться на юридических и физических лиц, учрежденных/находящихся за пределами ЕС, в том числе российских, обрабатывающих персональные данные субъектов персональных данных в ЕС в определенных Регламентом случаях.

Регламент детализирует либо устанавливает новые права субъектов персональных данных и обязанности лиц, обрабатывающих такие данные, а также меры ответственности, в том числе, административные штрафы за нарушение требований Регламента в размере до 20 миллионов евро либо до 4% от годового оборота.

Российским операторам персональных данных, чья деятельность подпадает под действие Регламента, необходимо до вступления его в силу принять необходимые организационные и технические меры, чтобы обеспечить соответствие положениям Регламента.

Оглавление

1 Территориальное действие

Контролеры и операторы, учрежденные в ЕС

«**Контролер**» для целей Регламента означает физическое или юридическое лицо, орган государственной власти, агентство или иное учреждение, которое самостоятельно или совместно с другими определяет цели и средства обработки персональных данных. (Например, врач-терапевт обычно является контролером данных своих пациентов; компания является контролером данных о своих клиентах и сотрудниках; спортивный клуб - контролером данных своих членов.)

«**Оператор**» означает физическое или юридическое лицо орган государственной власти, агентство или иное учреждение, которое обрабатывает персональные данные от имени контролера.

Регламент действует в отношении организаций, имеющих в ЕС «учреждения» (англ. establishment), где персональные данные обрабатываются «в контексте деятельности» такого учреждения, то есть независимо от того, на территории ЕС или нет фактически происходит обработка данных. Учреждение подразумевает эффективное и реальное осуществление деятельности посредством «стабильных договоренностей», независимо от их юридической формы - будь то через филиал или дочернее предприятие.

Определение «учреждения» в Регламенте, таким образом, соответствует определению, которое было дано Судом Европейского Союза («Суд ЕС») в деле Weltimmo в 2015 году V NAIH (C-230/14). Организация может быть «учреждена», когда она осуществляет «любую реальную и эффективную деятельность - даже минимальную» через «стабильные договоренности» в ЕС. Присутствия одного представителя может быть достаточно. Так, компания Weltimmo была признана имеющей «учреждение» в Венгрии в результате использования веб-сайта на венгерском языке, на котором рекламировалась недвижимость в Венгрии (это означало, что он считался «главным образом или полностью направленным на данное государство), использования местного агента (который отвечал за взыскание долгов и выступал в качестве представителя в административных и судебных разбирательствах), а также использования почтового адреса и банковского счета для деловых целей - несмотря на то, что Weltimmo была зарегистрирована в Словакии.

Организации, не учрежденные в ЕС, деятельность которых направлена на граждан ЕС

Такие организации будут подпадать под действие Регламента в случае, если они обрабатывают персональные данные субъектов персональных данных в ЕС в связи с:

- предложением им товаров или услуг (без требования оплаты); или
- мониторинга их поведения в ЕС.

Для предложения товаров и услуг (но не мониторинга), недостаточно чтобы Интернет-сайт был просто доступен в ЕС. Должно быть очевидно, что организация «предвидит», что ее деятельность будет направлена на субъектов персональных данных в ЕС.

Сами по себе доступность Интернет-сайта контролера, оператора или посредника в ЕС, адреса электронной почты или других контактных данных или использования языка, обычно используемого в третьей стране, где учрежден контролер, являются недостаточными для установления таких факторов. Вместе с тем, использование языка или валюты, обычно используемой в одном или нескольких государствах-членах с возможностью заказывать товары и услуги на таком языке или упоминание клиентов или пользователей, находящихся в ЕС, очевидно свидетельствуют о том, что контролер предусматривает предложение товаров или услуг субъектам персональных данных в ЕС.

Неясно, подпадают ли под действие Регламента организации, не учрежденные в государствах - членах ЕС, предлагающие товары и услуги юридическим (а не физическим) лицам в ЕС лицам.

«Мониторинг» включает отслеживание отдельных пользователей в Интернете для создания профилей, в том числе, когда это используется для принятия решений для анализа/прогнозирования личных предпочтений, поведения и отношения.

В то же время Регламент не применяется в случае обработки персональных данных физическим лицом в рамках «исключительно личной или домашней деятельности». Это касается переписки и ведения адресных книг, а также социальных сетей и онлайн-мероприятий, проводимых в социальных и домашних целях. Однако Регламент действует в отношении контролеров и операторов, которые «предоставляют средства для обработки", подпадающие под данное исключение.

2 Персональные данные

Для целей Регламента «персональные данные» означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); Идентифицируемое физическое лицо - это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайн идентификатор или один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности данного физического лица. Предусмотренный Директивой 95/46/ЕС критерий «все средства могут быть разумно использованы для идентификации» сохраняется.

В преамбуле к Регламенту подчеркивается, что определенные категории онлайн данных могут быть отнесены к персональным - онлайн идентификаторы, идентификаторы устройств, идентификаторы файлов cookie и IP-адреса. В октябре 2016 года Суд ЕС разъяснил статус динамических IP-адресов по делу Патрика Брейера против Германии (C-582/14), указав, что IP-адрес является персональными данными, когда принадлежит Интернет-провайдеру, но не представляет собой персональные данные, если они принадлежат стороне, у которой нет «средств, которые могут быть разумно использованы для идентификации личности».

При этом персональные данные, подвергшиеся псевдонимизации, которые могут быть отнесены к физическому лицу с использованием дополнительной информации, также будут считаться информацией об идентифицируемом физическом лице.

3 Представитель контролера или оператора, не учрежденного в ЕС

Контролер или оператор, не учрежденный в ЕС, обязан назначать представителя, если он обрабатывает персональные данные субъектов данных, находящихся в ЕС, и его деятельность по обработке связана с предложением товаров или услуг (независимо от того, взимается ли платеж с субъекта данных) таким субъектам данных или с мониторингом их поведения, поскольку их поведение имеет место в ЕС.

Исключения составляют случаи, когда:

- обработка осуществляется не на постоянной основе;
- обработка не ведется в больших масштабах, в отношении специальных категорий персональных данных или персональных данных, касающихся приговоров по уголовным делам и правонарушений; и

- обработка вряд ли приведет к риску причинения ущерба правам и свободам физических лиц с учетом характера, контекста, сферы применения и целей обработки; или
- контролер не является государственным органом.

Представитель должен находиться в одном из государств-членов ЕС, где находятся субъекты данных, чьи персональные данные обрабатываются.

Представитель должен действовать от имени контролера или оператора и любой надзорный орган должен иметь возможность обратиться к нему.

4 Отношения между контролером и оператором

Выполнение обработки оператором должно регулироваться договором или юридически обязывающим документом в соответствии с законодательством ЕС или государства-члена ЕС между оператором и контролером, определяющим предмет и продолжительность обработки, характер и цели обработки, тип персональных данных и категорий субъектов данных с учетом конкретных задач и обязанностей оператора в контексте выполняемой обработки и риска для прав и свобод субъектов данных.

Оператор не должен взаимодействовать с другим оператором без предварительного или общего письменного разрешения контролера.

Контролер или оператор должны вести учет операций по обработке, находящихся под его ответственностью. Каждый контролер и оператор обязаны сотрудничать с надзорным органом и делать эти записи по его запросу доступными для целей мониторинга таких операций по обработке.

Принимая во внимание современное состояние, затраты на реализацию и характер, сферу применения, контекст и цели обработки, а также риск причинения вреда правам и свободам физических лиц, контролер и оператор должны принимать соответствующие технические и организационные меры для обеспечения уровня безопасности, соответствующего рискам, включая, в частности:

- псевдонимизацию и шифрование персональных данных;
- обеспечение постоянной конфиденциальности, целостности, доступности и устойчивости систем обработки и услуг;
- способность своевременно восстанавливать доступность и доступ к персональным данным в случае физического или технического инцидента;
- процесс регулярного тестирования, оценки и оценки эффективности технических и организационных мер для обеспечения безопасности обработки.

Оператор обязан уведомить контролера без неоправданной задержки, узнав о нарушении персональных данных.

Если оператор нарушает требования Регламента, определяя цели и средства обработки, оператор считается контролером в отношении этой обработки и несет соответствующую ответственность.

5 Должностное лицо по защите данных

Контролер и оператор должны назначить должностное лицо по защите данных (ДЛ) (англ. data protection officer) в случае, если:

- обработка осуществляется государственным органом или учреждением (за исключением судов, действующих в рамках их полномочий); или
- основные действия контролера или оператора состоят (а) из операций по обработке, которые в силу своего характера, их объема и / или их целей требуют регулярного и систематического мониторинга данных в широких масштабах либо (б) в обработке в больших масштабах специальных категорий данных и персональных данных, относящихся к данным о судимости и правонарушениях.

«Регулярный и систематический мониторинг» включает все формы онлайн наблюдения и профилирования, в том числе для целей поведенческой рекламы и перенаправления сообщений по электронной почте, а также определения профиля заемщика и бальной оценки его платежеспособности, определения местоположения; мониторинг данных о состоянии здоровья и физической активности, скрытое видеонаблюдение, обработка подключенными устройствами (смарт-счетчики, умные автомобили и т. д.), маркетинговые активности, основанные на данных (т.н. «Большие данные»).

ДЛ должно обладать экспертными знаниями в области законодательства и практики защиты данных. Как указано в преамбуле Регламента, уровень экспертных знаний определяется, в частности, в соответствии с выполняемыми операциями по обработке данных и защитой, требуемой для персональных данных, обрабатываемых контролером или оператором.

Контролер или оператор должны:

- опубликовать контактные данные ДЛ и передать их в надзорный орган;
- обеспечить, чтобы ДЛ не получало никаких указаний по выполнению его функций.

ДЛ должно выполнять по меньшей мере следующие функции:

1) информировать и консультировать контролера или оператора и сотрудников, которые выполняют обработку персональных данных, об обязанностях в соответствии с Регламентом и другими положениями о защите данных действующими в ЕС или государствах-членах ЕС;
2) следить за соблюдением Регламента и другими положениями о защите данных ЕС или государств-членов и политикой контролера или оператора в отношении защиты персональных данных;
3) предоставлять консультации по запросу в отношении оценки воздействия защиты данных и контролировать ее эффективность;
4) сотрудничать с надзорным органом;
5) выступать в качестве контактного лица надзорного органа по вопросам, связанным с обработкой, и консультироваться, когда это необходимо, по любому другому вопросу.

Регламент позволяет назначать одно ДЛ на всю группу компаний при условии, такое лицо должно быть «легко доступно из каждой компании».

В случае, если ДЛ назначается на добровольной основе, назначивший его контролер или оператор должны соответствовать тем же требованиям, что установлены Регламентом для случаев обязательного назначения.

Если назначение ДЛ не является обязательным и ДЛ не назначается добровольно, иные сотрудники либо внешние консультанты могут назначаться для выполнения соответствующих функций.

6 Согласие на обработку персональных данных

Тогда как Директива 95/46/ЕС разрешает контролерам полагаться на неявное согласие и «отказ» (англ. opt-out) в некоторых обстоятельствах, Регламент устанавливает, что согласие должно быть дано четким утвердительным действием, означающим свободно предоставленное, конкретное, информированное и однозначное согласие субъекта данных на обработку персональных данных, касающихся его или ее, например, письменным заявлением, в том числе электронным способом, или устным заявлением.

Регламент прямо предусматривает, что согласие в письменной форме может быть предоставлено путем проставления «галочек» в форме на Интернет-сайте, выбора технических параметров для служб информационного общества или как другим заявлением или действием, ясно указывающим в этом контексте на принятие субъектом данных предлагаемой обработки его персональных данных.

Прямо выраженное согласие должно быть получено в следующих случаях:

- для обработки специальных категорий персональных данных, в частности, о расовой или этнической принадлежности, политических, религиозных или философских убеждениях или членстве в профсоюзах, генетических данных, биометрических данных с целью уникальной идентификации физического лица, данных о здоровье;
- на принятие решений относительно субъекта данных, «основанных исключительно на автоматизированной обработке, включая профилирование»;
- на передачу персональных данных в страны, которые не обеспечивают достаточный уровень защиты, если другой механизм передачи не установлен.

Согласие должно охватывать все виды обработки, осуществляемые с одной целью или целями. Когда обработка имеет несколько целей, необходимо получение согласия на все из них. Ожидаются дальнейшие официальные разъяснения данных положений, однако контролерам и операторам, на которых распространяется действие Регламента, необходимо пересмотреть существующие механизмы получения согласия, с тем, чтобы они обеспечивали возможность субъектам данных давать подлинное и детализированное согласие.

Субъект данных имеет право отозвать свое согласие в любое время. Контролеры должны информировать субъектов данных о праве на отзыв до получения их согласия. После того, как согласие будет отозвано, субъекты данных имеют право требовать удаления своих персональных данных и прекращения их использования для обработки.

Регламент содержит специальные положения в отношении обработки персональных данных несовершеннолетних. Если услуги информационного общества предлагаются непосредственно ребенку, обработка персональных данных ребенка является законной, если ему или ей исполнилось 16 лет. В отношении детей младше 16 лет согласие на обработку предоставляется или разрешается лицом, осуществляющим функции родителя.

7 Меры по защите персональных данных

Впервые на законодательном уровне Регламент вводит понятие «**защита данных по проекту**» (англ. data protection by design). На концептуальном уровне защита данных по проекту означает, что конфиденциальность должна быть отличительной чертой на стадии разработки продукта (решения в сфере информационных технологий, а не внедряться в него позднее. Регламент устанавливает общую обязанность контролеров как во время определения средств для обработки, так и во время самой обработки персональных данных принимать надлежащие технические и организационные меры с учетом «уровня техники и

затрат на реализацию» и «характера, сферы применения, контекста и целей обработки, а также риска меняющейся вероятности и существенности для прав и свобод физических лиц».

Однако в отличие от Директивы 95/46/ЕС, Регламент содержит конкретные предложения о том, какие виды мер безопасности могут считаться «соответствующими риску», в том числе:

- псевдонимизация и шифрование персональных данных;
- способность обеспечить постоянную конфиденциальность, целостность, доступность и устойчивость систем обработки и услуг;
- возможность своевременного восстановления доступности и доступа к персональным данным в случае физического или технического инцидента;
- процесс регулярного тестирования, оценки и оценки эффективности технических и организационных мер для обеспечения безопасности обработки.

Контролер должен применять соответствующие технические и организационные меры для обеспечения того, чтобы по умолчанию обрабатывались только персональные данные, необходимые для каждой конкретной цели обработки. Это обязательство распространяется на объем собранных персональных данных, степень их обработки, период их хранения и их доступность. В частности, такие меры должны гарантировать, что по умолчанию персональные данные не становятся доступными неограниченному числу физических лиц без человеческого вмешательства.

Регламент вводит также новое для права ЕС понятие «**псевдонимизация**» (англ. pseudonymization) - обработка персональных данных таким образом, что они больше не могут быть отнесены к конкретному субъекту данных без использования дополнительной информации при условии, что такая дополнительная информация хранится отдельно и подлежит техническим и организационным мерам с тем, чтобы персональные данные не были отнесены к идентифицированному или идентифицируемому физическому лицу.

Псевдонимизация, таким образом, может значительно снизить риски, связанные с обработкой персональных данных, поддерживая при этом их полезность. По этой причине отдельные положения Регламента создают стимулы для контролеров для псевдонимизации данных, которые они собирают.

8 Информирование субъектов данных

Регламент расширяет объем информации, которую контролер должен предоставить субъектам данных перед сбором персональных данных. В дополнение к наименованию контролера, целям обработки и любым получателям персональных данных, контролеры должны информировать субъектов данных о: сроке хранения данных; праве отозвать согласие в любое время, праве запрашивать доступ, исправление или ограничение обработки и праве подавать жалобу в надзорный орган. Данная информация должна раскрываться в ясной и легкодоступной форме, с использованием понятного и простого языка, который подходит для соответствующей аудитории.

Для контролеров, которые получают данные от источника, отличного от субъекта данных, от другого контролера или общедоступной записи, раскрытие информации не требуется, если для этого потребуется «непропорциональное усилие».

Регламент обязывает контролеров общаться с субъектами данных «в сжатой, прозрачной, понятной и легкодоступной форме, используя понятный и простой язык». Если субъект данных стремится реализовать одно из прав, предоставленных Регламентом, контролер должен предпринять соответствующие действия без неоправданной задержки или не

позднее, чем через месяц после запроса. Однако контролер вправе на продление данного срока в случае необходимости из-за большого количества запросов. Если контролер не желает отвечать на запрос, он должен объяснить свое решение субъекту данных в течение одного месяца. Все эти услуги должны быть бесплатными, если только запросы не являются явно необоснованными или чрезмерными.

Регламент предусматривает право контролера отказаться от действия по запросу, если он продемонстрирует, что он не в состоянии идентифицировать субъекта данных. С другой стороны, если у контролера есть разумные сомнения относительно личности лица, делающего запрос, он может попросить у него дополнительную информацию, чтобы подтвердить его личность.

9 Профилирование

Регламент вводит понятие «**профилирования»** (англ. profiling) - автоматизированной обработки персональных данных в любой форме, при которой оцениваются личные аспекты, связанные с физическим лицом, в частности для анализа или прогнозирования аспектов, касающихся работы субъекта данных, его или ее экономического положения, здоровья, личных предпочтений или интересов, его или ее надежности или поведения, местонахождения или передвижений, когда такая обработка создает юридические последствия для него или ее или аналогично оказывает существенное влияние на него или нее.

Субъект данных должен быть специально уведомлен об осуществлении профилирования и его последствиях и вправе в любое время заявить возражение в связи с таким профилированием.

Принятие решений на основе такой обработки, допустимо в тех случаях, когда:

- это прямо разрешено законодательством ЕС или государства-члена, к которому относится контролер, в том числе для целей мониторинга и предотвращения мошенничества и уклонения от уплаты налогов, а также обеспечения безопасности и надежности обслуживания, предоставляемого контролером, или
- необходимо для заключения или исполнения контракта между субъектом данных и контролером, или
- субъект данных предоставил его или ее прямо выраженное согласие.

В любом случае, контролер должен обеспечить, чтобы такая обработка осуществлялась с надлежащими гарантиями, включающими предоставление конкретной информации субъекту данных, его право на участие человека при принятии решений, на выражение своей точки зрения, на получение разъяснения решения, принятого на основе такой оценки и оспаривание решения.

10 Трансграничная передача данных

Регламент устанавливает ограничения на передачу персональных данных в «третьи страны» (т. е. за пределы ЕС) и в международные организации.

Передача персональных данных в третью страну или международную организацию может осуществляться без необходимости получения разрешения при условии, что Европейская комиссия (далее - «Комиссия») приняла решение о том, что третья страна, территория или один или несколько секторов в пределах этой третьей страны, или соответствующая международная организация обеспечивают адекватный уровень защиты персональных данных («решение о достаточности»). Действующий перечень стран, которые ранее

утверждены Комиссией, включает: Андорра, Аргентина, Канада (где применяется PIPEDA), Швейцария, Фарерские острова, Гернси, Израиль, остров Мэн, Джерси, Восточная Республика Уругвай и Новая Зеландия.

В отсутствие решения о достаточности контролер или оператор должны принять меры для компенсации отсутствия защиты данных в третьей стране путем предоставления соответствующих гарантий субъекту данных и при условии, что доступны эффективные средства правовой защиты прав субъекта данных, в том числе:

1) юридически обязывающий и подлежащий исполнению документ между государственными органами соответствующих стран;
2) обязательные корпоративные правила, утвержденные компетентным надзорным органом;
3) положения о стандартной защите данных, принятые Комиссией; или
4) положения о стандартной защите данных, принятые надзорным органом и одобренные Комиссией;
5) утвержденный кодекс поведения вместе с обязательными и подлежащими исполнению обязательствами контролера или оператора в третьей стране применять соответствующие гарантии, в том числе в отношении прав субъектов данных; или
6) утвержденный механизм сертификации вместе с обязательными и подлежащими исполнению обязательствами контролера или оператора в третьей стране применять соответствующие гарантии, в том числе в отношении прав субъектов данных.

В случае отсутствия решения о достаточности или надлежащей гарантии трансграничная передача персональных данных может осуществляться только на одном из следующих условий:

1) субъект данных прямо согласился с предлагаемой передачей после того, как был проинформирован о возможных рисках таких передач для субъекта данных из-за отсутствия решения о достаточности и соответствующих гарантий;
2) передача необходима для договора между субъектом данных и контролером или осуществления преддоговорных мер, принятых по запросу субъекта данных;
3) передача необходима для заключения или исполнения договора, заключенного в интересах субъекта данных между оператором и другим физическим или юридическим лицом;
4) передача необходима по важным причинам в общественных интересах;
5) передача необходима для установления, осуществления или защиты исковых требований;
6) передача необходима для защиты жизненно важных интересов субъекта данных или других лиц, если субъект данных физически или юридически неспособен дать согласие.

Следует отметить, что нарушение положений о Регламента о трансграничной передаче данных может повлечь административный штраф в максимальном размере (до 4% общемирового годового оборота).

11 Оценка воздействия при защите данных

Оценка воздействия при защите данных должна проводиться контролером до обработки, чтобы оценить конкретную вероятность и существенность риска для прав и законных

интересов субъектов данных, с учетом характера, объема, контекста и целей обработки и источников риска.

В обязательном порядке такая оценка должна проводиться в следующих случаях:

1) персональные данные обрабатываются для принятия решений относительно конкретных физических лиц после любой систематической и обширной оценки личных аспектов, связанных с физическими лицами, на основе профилирования этих данных или после обработки специальных категорий персональных данных, биометрических данных или данных о судимости и правонарушениях или связанных с ними мерами безопасности;

2) мониторинг общественных мест в широких масштабах, особенно при использовании оптико-электронных устройств или для любых других операций, когда компетентный надзорный орган считает, что обработка, вероятно, приведет к высокому риску для прав и свобод субъектов данных;

3) крупномасштабные операции по обработке значительного объема персональных данных на региональном, национальном или наднациональном уровне, которые могут повлиять на большое количество субъектов данных и привести к высокому риску, в рамках которых в соответствии с достигнутым уровнем технологических знаний в широких масштабах используется новая технология, а также другие операции по обработке, которые создают высокий риск для прав и свобод субъектов данных.

Оценка воздействия должна включать по меньшей мере:

- систематическое описание предполагаемых операций обработки и целей обработки, в том числе, когда это применимо, законные интересы контролера;
- оценку необходимости и пропорциональности операций по обработке в отношении целей;
- оценку рисков для прав и свобод субъектов данных; а также
- меры, предусмотренные для устранения рисков, включая меры предосторожности, меры безопасности и механизмы для обеспечения защиты персональных данных и для подтверждения соблюдения Регламента с учетом прав и законных интересов субъектов данных и других заинтересованных лиц.

12 Уведомление о нарушениях персональных данных

В соответствии с Регламентом нарушением персональным данных является нарушение безопасности, приводящей к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к переданным, хранящимся или иным образом обрабатываемым персональным данным.

По сравнению с Директивой 95/46/ЕС, Регламент устанавливает новый режим уведомления в случае нарушения персональным данных.

Оператор обязан уведомить контролера о нарушении без ненадлежащего промедления.

Контролер обязан уведомить надзорный орган о нарушении без ненадлежащего промедления, в течение 72 часов, если это возможно, за исключением случаев, когда нарушение не может создать существенный риск для прав и законных интересов физических лиц.

Контролер также обязан уведомить о нарушении без ненадлежащего промедления субъектов данных, если нарушение может создать существенный риск для их прав и законных интересов, за исключением случаев, когда:

1) контролер принял соответствующие технические и организационные меры защиты, которые делают данные непонятными для любого лица, которое не имеет доступа к нему, например шифрование;

2) контролер предпринимает действия после нарушения персональных данных для обеспечения того, чтобы высокий риск для прав и свобод субъектов данных вряд ли осуществился;

3) когда уведомление каждому субъекту данных будет сопряжено с непропорциональными усилиями, и в этом случае могут использоваться альтернативные методы коммуникации.

Несоблюдение данных требований Регламента влечет ответственность в форме административного штрафа в размере до 10 миллионов евро или в отношении организаций - до 2% от общемирового годового объема выручки предыдущего финансового года, в зависимости от того, что больше.

13 Права субъектов персональных данных

A. Право на доступ

Регламент по сравнению с Директивой 95/46 /ЕС устанавливает более детализированное право на доступ. Пользователи вправе запросить копию своих персональных данных, подлежащих обработке, а также информацию о целях обработки, периоде времени, в течение которого будут храниться данные, личность любых получателей данных, логика автоматической обработки данных и последствия любого профилирования. Контролерам необходимо будет настроить процессы для ответа на запросы о предоставления доступа и, в частности, для проверки личности субъекта данных, который запрашивает доступ. В тех случаях, когда контролер обрабатывает «большое количество информации» о субъекте данных, он вправе потребовать, чтобы субъекты данных указывали конкретные данные или деятельность по обработке, о которых идет речь в запросе.

B. Право на исправление

Субъект данных имеет право потребовать от контролера без неоправданной задержки исправления неточных персональных данных, касающихся его или ее. Принимая во внимание цели обработки, субъект данных имеет право на дополнение персональных данных, являющихся неполными, в том числе путем предоставления дополнительного заявления.

C. Право на возражение

Субъект данных имеет право возражать по основаниям, касающимся его или ее конкретной ситуации, в любое время в отношении обработки персональных данных, касающихся его или ее (а) для выполнения задачи, выполняемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контролера, или (б) для целей законных интересов контролера или третьего лица, за исключением случаев, когда основные права и свободы субъекта данных превалируют над такими интересами или, требуют защиты персональных данных, в частности, когда субъектом данных является ребенок.

Контролер в таком случае обязан прекратить обработку персональных данных, если контролер не предоставит убедительные законные основания для обработки, которые превалируют над интересами, правами и свободами субъекта данных или для создания, осуществления или защиты исковых требований.

D. Право на удаление

В отличие от Директивы 95/46 /ЕС, Регламент прямо признает «право на удаление» (англ. right to erasure), которое представляет собой расширенный вариант так называемого «права на забвение», признанного Европейским судом в деле Google Spain v AEPD и Марио Костея Гонсалес 2014 года. В решении суд потребовал от поисковых систем по просьбе физического лица удалять ссылки на веб-страницы, которые появляются при поиске имени этого лица, если только «преобладающая заинтересованность широкой общественности» в доступе к информации не оправдывает отказ поисковой системы удовлетворять запрос.

Контролеры должны удалять персональные данные без неоправданной задержки при наличии одного из следующих оснований:

1) персональные данные больше не нужны в отношении целей, для которых они были собраны или обработаны иным образом;
2) субъект данных отозвал согласие, на котором основана обработка, и где нет другого юридического основания для обработки;
3) субъект данных возражает против обработки, и нет никаких законных оснований для обработки, или субъект данных возражает против обработки персональных данных для целей прямого маркетинга;
4) персональные данные были незаконно обработаны;
5) персональные данные должны быть удалены в целях исполнения обязанности предусмотренной законодательством ЕС или государства-члена, которому подчиняется контролер;
6) персональные данные были собраны в связи с предложением услуг информационного общества непосредственно ребенку.

E. Право на ограничение

Субъект данных имеет право требовать «ограничения обработки» на время, необходимое для проверки достоверности информации, если он оценивает ее точность, а также в случаях, когда контролер больше не нуждается в данных, но субъект данных нуждается в них для судебного иска и когда субъект данных возражает против обработки, но контролер стремится доказать, что он имеет законные основания для преодоления возражения.

Если субъект данных запрашивает ограничение обработки, контролер должен временно удалить данные из общей системы регистрации или с общедоступного веб-сайта, чтобы избежать дальнейшей обработки.

F. Право на портативность

В тех случаях, когда операторы обрабатывают персональные данные с помощью «автоматизированных средств», субъектам данных Регламент предоставляет право:

1) получать касающиеся их персональные данные в «структурированном, обычно используемом, машиночитаемом и совместимом формате»,
2) передавать такие данные другому контролеру или

3) требовать, чтобы их персональные данные были переданы непосредственно от одного контролера на другому, при условии, что такая передача является «технически осуществимой».

В отношении контролеров Регламентом установлены корреспондирующие обязанности по предоставлению и передаче данных в соответствующем формате. Однако в преамбуле к Регламенту указано, что он не налагает обязанность на контролеров внедрять для этих целей технологические системы, которые являются технически совместимыми.

14 Контроль за соблюдением Регламента. Средства правовой защиты

Каждое государство-член ЕС обязано назначить один или несколько независимых государственных органов ответственным(и) за контроль за соблюдением Регламента в целях защиты основных прав и свобод физических лиц в отношении обработки и облегчения свободного обращения персональных данных в рамках ЕС («надзорный орган») и уведомить об этом Комиссию до 25 мая 2018 г.

Надзорный орган государства основного или единственного места учреждения контролера или оператора будет уполномочен действовать в качестве ведущего надзорного органа для целей трансграничной обработки, осуществляемой этим контролером или оператором.

Надзорный орган будет иметь, в частности, следующие полномочия:

1) проводить расследования в форме проверок защиты данных;
2) получить доступ к любым помещениям контролера и оператора, в том числе к любому оборудованию и средствам обработки данных, в соответствии с процессуальным законодательством ЕС или государства-члена.
3) выдавать предупреждения и выносить выговоры контролеру или оператору, осуществляющим операции по обработке, которые могут нарушать положения Регламента;
4) давать указания контролеру или оператору привести операции по обработке в соответствие с положениями Регламента, если это необходимо, в определенном порядке и в течение определенного периода времени;
5) наложить временное или окончательное ограничение, включая запрет на обработку персональных данных;
6) налагать административный штраф в дополнение к или вместо вышеуказанных мер в зависимости от обстоятельств каждого отдельного дела.

Субъекты персональных данных, чьи данные обрабатывается не в соответствии с Регламентом, имеют право подавать жалобы в надзорные органы, а такие органы обязаны информировать субъектов о ходе и результатах рассмотрения жалоб.

Как субъекты данных, так и другие заинтересованные лица вправе обращаться в суд (имеют право на эффективное судебное средство правовой защиты) в связи с определенными актами и решениями надзорных органов:

- любое лицо - в отношении юридически обязательных решений, касающихся его или ее, принятых надзорным органом.
- субъекты персональных данных - в случае, если надзорный орган не рассматривает жалобу или не информирует субъекта данных в течение 3 месяцев о ходе или результатах рассмотрения его или ее жалобы.

Субъекты данных, права которых были нарушены, имеют право на обращение в суд с иском против контролера или оператора персональных данных ответственного за предполагаемое нарушение.

Любое лицо, получившее ущерб в результате нарушения Регламента, имеет право на получение компенсации от контролера или оператора.

Ответственность между контролерами и операторами распределяется следующим образом:

- контролеры несут ответственность за ущерб, вызванный обработкой персональных данных, не соответствующей Регламенту;
- операторы несут ответственность только за ущерб, причиненный любым видом обработки в нарушение обязательств, прямо налагаемых на операторов Регламентом или вызванных внешней обработкой либо противоречащей правомерным инструкциям контролера;
- контролеры и операторы, которые участвуют в одной и той же обработке персональных данных, несут ответственность за любой ущерб полном объеме. Однако оператор или контролер, который несет ответственность за выплату возмещения ущерба, вправе взыскать возмещение с других соответствующих сторон в части, соответствующей их части ответственности за ущерб.

При этом Регламент прямо устанавливает, что компенсация может быть взыскана в отношении как оцениваемых в денежной форме убытков, так и не оцениваемого в денежной форме ущерба.

15 Административные штрафы

Надзорные органы вправе налагать значительные административные штрафы на контролеров и операторов данных, вместо или в дополнение к иным мерам реагирования на нарушения, которые находятся в компетенции надзорных органов.

В случае незначительного нарушения или если штраф возлагает непропорциональное бремя на физическое лицо, вместо штрафа надзорный орган может объявить выговор.

Регламент предусматривает два пороговых значения размеров штрафов в зависимости от видов нарушений.

Нарушение следующих положений повлечет административные штрафы **до 20 миллионов евро или до 4% мирового годового оборота**, в зависимости от того, что больше:

- основные принципы обработки, включая условия для согласия (статьи 5, 6, 7 и 9 Регламента);
- права субъектов данных (статьи 12-22 Регламента);
- трансграничная передача (статьи 44-49 Регламента);
- обязательства по законам государств-членов, принятые в соответствии с Главой IX Регламента;
- несоблюдение порядка, установленного надзорными органами или несоблюдение в рамках расследования надзорного органа в соответствии со статьей 58 (1) Регламента.

Остальные нарушения повлекут административные штрафы **до 10 миллионов евро или, в случае компаний, до 2% от годового мирового оборота**, в зависимости от того, что больше. В частности, нарушение следующих обязанностей в соответствии с Регламентом:

- получение согласия на обработку данных, относящихся к детям (статья 8);
- внедрение технических и организационных мер для обеспечения защиты данных по проекту и по умолчанию (статья 25);
- совместных контролеров согласовать их соответствие требованиям Регламента (статья 26);
- контролеров и операторов, не учрежденных в ЕС, по назначению представителей (статья 27);
- контролеров в связи с привлечением операторов (статья 28);
- операторов по привлечению субподрядчиков только с предварительного согласия контролера и обработке данных только на основании инструкций контролера (статьи 28-29);
- ведение учета операций по обработке персональных данных (статья 30);
- контролеров и операторов сотрудничать с надзорными органами (статья 31);
- внедрение технических и организационных мер (статья 32);
- сообщение о нарушениях персональных данных в случаях, установленных Регламентом (статьи 33-34);
- проведение оценки воздействия при защите данных (статьи 35-36);
- назначение ДЛ (статьи 37-39).

Если Регламент не устанавливает административные штрафы за какие-то нарушения, государства-члены ЕС обязаны принять свою систему штрафов и уведомить Комиссию о любых соответствующих законодательных изменениях.

****

С уважением,

Юридическая фирма GRATA International (Москва)

Информация выше имеет обзорный характер и не является юридической консультацией. Данная информация подготовлена с целью уведомления наших клиентов и других заинтересованных лиц о нововведениях и может содержать ссылки на Интернет сайты помимо сайта GRATA International. На основании данной информации не следует осуществлять какие-либо действия в конкретной ситуации без надлежащей юридической консультации.

Предоставляемые GRATA International услуги включают, в частности:

- разработку необходимых организационно-распорядительных документов по защите персональных данных и коммерческой тайны;
- подготовку уведомлений об обработке персональных данных представляемых в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);
- консультирование по вопросам локализации баз данных персональных данных в России, трансграничной передачи персональных данных и иным вопросам;
- консультирование по вопросам соблюдения требований Общего регламента по защите данных российскими операторами персональных данных;
- представление интересов в ходе проверок Роскомнадзора.

Контакты для дополнительной информации:

Яна Дианова

Директор Департамента корпоративного и коммерческого права GRATA International (Москва)

Т.: +7 (495) 660 11 84

E.: Ydianova@gratanet.com